A Secure Intrusion Prevention Protocol for VANET to Enhance Security

J.Veneeswari[1], C.Balasubramanian[2]
1 PG-Scholar, Department of CSE, PSRRengasamy College of Engineering for Women, Sivakasi,
2Professor- Department of CSE, PSRRengasamy College of Engineering for Women, Sivakasi.
E-mail:-venijeyaraj93@gmail.com,c.balasubramanian@gmail.com,

ABSTRACT *A vehicular ad-hoc network (VANETs) is emerging technology in wireless ad-hoc network.VANETs are dope out to improve vehicular safety and manage the traffic in the urban areas. Adaptive slot assignment strategy with fuzzy logic are used with multipath routing mechanism with TDMA allocation to limit the collision rate and improve the energy and reduce stoppage in the vehicle statement. In this paper, an interruption avoidance protocol that are integrated with digital signature and game theory approach with Road side unit control to enhance the security and protecting the VANET environment. Using this intrusion prevention protocol is implemented to examine the various parameter values to provide the Quality of Service, inter –vehicle and intra-vehicle security in the zone with security showed with the simulated results.*

I. INTRODUCTION

VANET environment are developed with the Intelligent Transportation system for fast and intelligent means of communication with the Distributed database multipath routing and collision avoidance technique.ASAS-fuzzy logic are taken with the routing to provide TDMA based allocation with various vehicles in urban road .VANET provide the safety and reduces the accident with improve the safety measures of the vehicle to limit the accident and it claims the noteworthy information to vehicle, roadside unit ,for authenticated environment. User authentication increases the accessing information with secured confident level of the user. Various authentication protocols are deployed in the road and vehicles.

IETF has standard network mobility provide the stability to provide the various data service with global connectivity of vehicles with the data services.VANET with pure ad hoc network where vehicle to vehicle without any need of centralized control of any infrastructure. Next to that Road side unit (RSU)with the fixed content are used these both are provide with security to avoid the steeling of information.CAR-2-CAR consortium has developed many security protocols to crash the attackers when the frequent exchange of data on vehicles in the security. Destination based on the distance vector routing is used in the basic with multiple attacker avoidance is stated in SEAD (secure and efficient Adhoc distance vector) .It intake more bandwidth and limited CPU processing its more capable to protect the DOS attack. It works with the help of hash function by choosing the random values at initial. Discovering the initial route which disperse the each outgoing with encoded scheme .SMT(secure message transmission)protocol with the light weight active path communication in this protocol it sends the acknowledgement to both sender and receiver vehicle. To protect the location information they develop the NDM (Non-Disclosure method) it covers the Information disclosure, location tracking with technology of asymmetric cryptography is used it provide the security requirement privacy .ARIDANE it terminate the route of uncompromised node. it covers the DOS,routing attack, replay attack with the symmetric cryptography, MAC it gives authentication to each vehicles. Cryptosystem are used with the privacy of message exchange and privacy with multilayer attack FHSS (frequency –hopping spread spectrum) is used in the bodily coating to avoid the DOS attack in vehicles.

II. RELATED WORK

The system proposed in [4] it is a impact of the mobility on the transmit of overhaul with the efficient MAC protocol it leads to the development of inter-vehicle communication through various monitoring mechanism. Reliable Reservation (RR-allocation) is capable for transmit the slotted/framed for their broadcast service it is provided with TDMA based allocation.RR-allocation provide an reliable broadcast service and reservation of access channel avoid the collision and eliminate parallel transmission. Broadcasting vehicles belong on various terminals they do not know each other vehicle for concurrent transmission. The transmission causes collision by uncovered vehicles that lead to hidden terminal

Problem. Clustering method is intense technique to reduce the collision in transmission is used in[5].Directional stability based clustering algorithm(DISCA) is used for maintain the stability of the cluster with the mobility of the vehicle and direction of mobility in vehicles and reduce the time to reform the cluster again.The clustering

efficiency is based on the active cluster that are present prolong time in medium. Mobility based of clustering is proposed in[6]it provide the stable cluster with high mobility of vehicles. Based on cluster formation it elect the cluster head for message transmission it maintain availability to provide the self recognizing of vehicle with mobility based ad-hoc clustering scheme(MOBIC).Space –orthogonal frequency(SOFT) is provide with the medium layer with Time access control for VANET(SOFT-MAC) are used to provide secure interaction between two transmitter in[7]they proposed to enhance the QOS requirement to reduce the collision overhead here we can use the more number of vehicles .Vehicular multichannel MAC protocol (VE-MAC) proposed in [8] is centralized manner with control of allocated time slots are used to provide limited access of cluster to reduce probability ratio of collision. Adaptive TDMA slot assignment protocol (ATSA) in[8] this allocate the time slots based on the mobility of the vehicles with correct direction and location of the vehicle it reduce the vehicle that access the same time slot it reduce the collision of redundant access of the vehicle.
The proposal of [9] specified with the technique named as Adaptive slot assignment strategy (ASAS) which provide the timeslot for access the communication channel based on the cluster head elected on the vehicle to minimize the collision in vehicles .In various solution scheme used for vehicles to avoid these type of access and merging collision in the network. It allow one vehicle to transmit in the particular time slot based on the request. This schedule of time slot is tabulated with the cluster head formation.warmhole attack is taken in the network . Nash Equilibrium (NE) game which provide the channel allocation security issues are arise the network found and resolved.

III. PROBLEMS

In VANETs without incorporating security in fuzzy logic to make the VANET enivironment with more risk many packet delay ,energy drop can occur in the network.Our proposed paper is taken with the warmhole attack is taken in the ASAS-FUZZY network and build with the digital signature and game theory approach to increase the energy ,limits the delay , packet drop network over head is reduced for the vehicles in the urban areas.

IV. SYSTEM DESCRIPTION

4.1 InVANET(Intelligent Vehicular AdhocNetwork)

- Intelligent vehicular network are concentrate the communication that are based on the vehicles –vehicles and vehicles –roadside unit.
- Decision making taken through various inferences in traffic.
- It increase the dynamic mobility of the vehicle with the increase of high speed communication and road safety.

FIG:-1 INTELLIGENTVEHICULAR ADHOC NETWORK

VANET COMMUNICATION METHODS

In urban areas there are large number of vehicles.There are more than 750 million of vehicles having Vehicular network system.Information sharing is very important between the vechicles.Using DSRC vehicles take place in the communication range of communication is reached around the signal up to 1 km with independent manner.Intelligent transport system (ITS) broadcast messages to other vehicle which connect the network devices.

The ITS play main role of passing the information each vehicle with safe destination with collision avoidance.It coordinate the vehicles through the transporation or location of each vehicle in the urban area.

FIG 2:-VANET COMMUNICATION

Each events that occur in the environment that shows in fig [1] are passed to other vehicle for the vehicle safety

4.2 TDMA ALLOCATION:-

TDMA allocation is offered with the various slot allocation and reservation to provide the service to channel in the vehicles that are requested.

- TDMA slot assignment- Vehicles position are monitored with a global positioning system(GPS) to allocate the time
- TDMA slot reservation-It based on the vehicles that requested to cluster head

FIG:-3 TDMA SLOT ASSIGNMENT AND RESERVATION

In fig:-2 the cluster is dope out with the more vehicles with the reserved time slot for each cluster head to transmit the information to another cluster head. Transformation of mobility information is passed by the vehicles that are monitored the information by the presence of Global positioning system (GPS) to know the location .

4.3 ASAS PROTOCOL

Adaptive slot assignment strategy (ASAS) is technique used in this paper to allocate the particular access of the vehicle that are processed to reserve the time slot for multiple request given by the vehicles for their interactions that are requested by the vehicles, with the acceptance of the high priority of the messages that depends upon the speed, location. It minimize the inter cluster formation of the vehicle and improve the throughput for each vehicle

Service channel (SCH) offers the service for an efficient channel to access frequently with time slots and to minimize the collision rates in different speed conditions by their given request.

4.4 FUZZY LOGIC

A group of fuzzy rules like human brain which predict the values for interpretation of uncertain sensory information that given by the vehicle

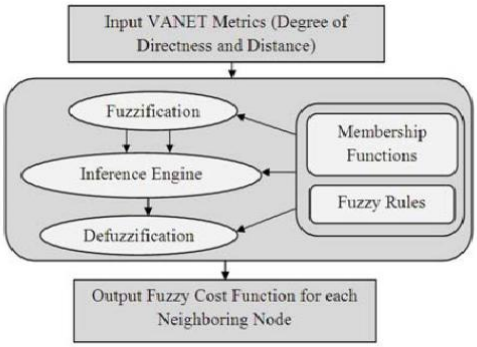


FIG :-4 FUZZYCOST LOGIC FOR FORWARDING PACKET

In degree of fuzzy cost is determined by the given inputs that are fuzzified to provide appropriate output with the range of vehicles and the direction of vehicle for the communication.

$$DISTRANCE=1-\frac{DFV}{RFV} \quad \text{..... (1)}$$

DFV=Direction of vehicle
RFV=Range of vehicle
In this equation (1) that are needed to calculate the distance of the vehicles. Using the distance we can calculate the distance of parameter value.

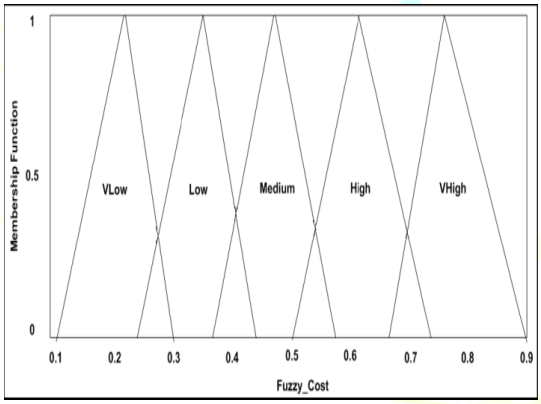


FIG-: 5 OUTPUT PARAMETER FOR FUZZY LOGIC

In fig 4 there are various output parameter that measured by the various fuzzy cost and membership functions.

4.5 SECURITY REQUIREMENT FOR VANET

The secure VANET environment with the enhancing speed with reducing the adversaries in VANET

- Authentication
- Availability
- Non-repudiation
- Privacy
- Real time constraints
- Integrity
- Confidentiality

Preserving the information from the unauthorized persons. Keys infrastructure is used to update the security in vehicle. License fed in to the Road Side Unit (RSU) to recognize the vehicle identity, location, driver information and which direction the vehicle are travelling .Temporary keys are used to preserve the safety in the identity. Vehicle acknowledgement is important for the real time constraints. Prevention of data security to alter

the data content from the hackers after the attack it retrieved the message from the receiver end within the milliseconds.

Threats to Availability, Authenticity and Confidentiality

Many threats are happen in the routing in the vehicle to vehicle and infrastructure.

- Denial of service Attack
- Broadcast Tampering
- Malware
- Spamming
- Black hole attack

The attack renders the network unavailable to authentic user for serious disruption to its operation. Malware attacks are more likely to carried attackers in insider and outsider with the surplus data.

V. NETWORK MODEL

In this proposed system the network model of the VANET are the base for the network model is to create the mobility nodes in the environment and with the topology specification to reach the destination. In the urban traffic area are consider in the system to monitor the range of collision avoidance.

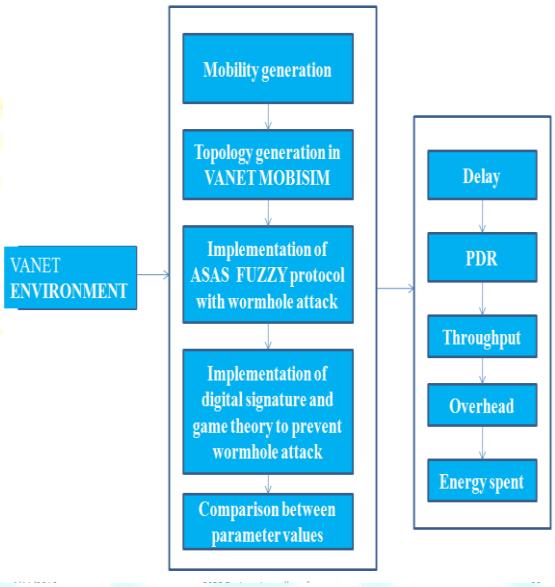


FIG 6:-IMPLEMENTATION OF THE SECURITY IN VANET ENVIRONMENT

QOS parameter are evaluated in the security VANET environment with the deploymentation of VANETMOBISIM topology to reduce the delay for the intervehicle message transmission.

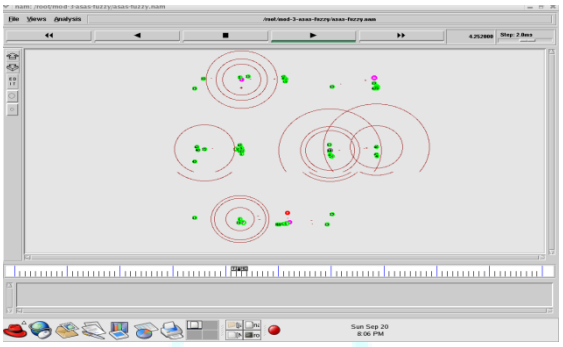
VI. IMPLEMENTATION

Deploying this work is first to create the mobility node with the network simulator .In this routing protocol are used to measure the QOS parameters.

- Node implementation in ASAS-FUZZY with wormhole attack
- Implementing digital signature and game theory approach
- Comparison between wormhole attack with ASAS FUZZY approach and enhanced ASAS FUZZY with game theoretic approach and digital signatures .

6.1 NODE IMPLEMENTATION IN ASAS- FUZZY WITH WORMHOLE ATTACK

Nodes are implemented in the topology in VANETMOBISIM . Creation of nodes is base for VANET and transfer of packets between nodes. Using TCL script to verify the nodes.it is used with ASAS-FUZZY protocol .



SCREEN SHOT :-1 ASAS –FUZZY PROTOCOL

In this we can calculate the collision rate, delay, energy spent and through put ratio.

TOPOLOGY GENERATION:-

Road topology with number of vehicles 50 is created using Vanetmobsim and output of VANET **is** fed as input to ns2 fo rmobility of nodes**.**Integrating VANET.Jar with road map file to form mobility

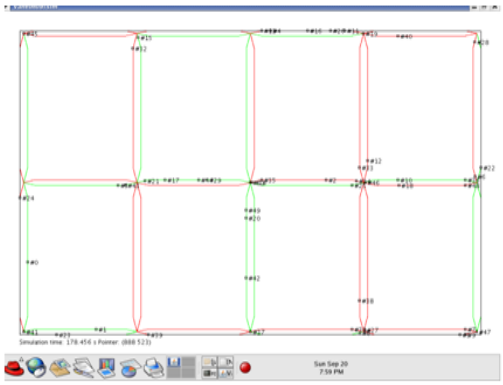
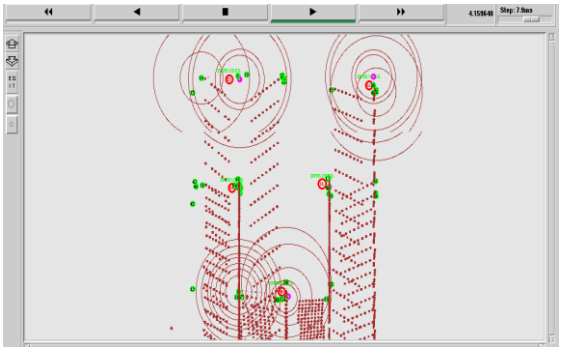


FIG:-7 VANETMOBISIMTOPOLOGY GENERATION

In FIG:-6 road topology is generated with the road map files. Integrating VANET.Jar with road map to form mobility files are fed to ASAS implementation.

WARMHOLE ATTACK:-

Formation of the VANET MOBI SIM topology in the urban road with fuzzy based rules to inhibit the wormhole hole attack in that malicious nodes are formed in the network to form a tunnel like structure to steal the privacy of original routing information .Original certainty of information are taken and content are modified to cause more problem in the deployed nodes with the fuzzy logic in the network. Denial of service are happen in the vehicle causes more delay of message transmission and reduce the ratio of packet transmission in multiple routing.



SCREEN SHOT :-2 WORM HOLE ATTACK

Wormhole attack with ASAS FUZZY-Protocol is deployed in the network and it degraded the performance. Service taken in the each nodes with the loss of energy, false data reaches the destination end. During the routing in this node deployment causes more collision in the network .

CALCULATION:-

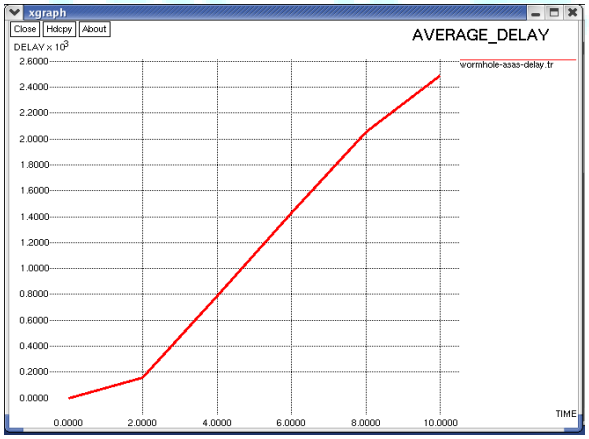
- **Delay=End time-Start time**
- **Collision rate =**

$$\frac{\text{Number of packet recevied}}{\text{Number of packet send}}$$

- **Consume energy = Inital energy – Final energy**
- **Total energy=Total consume energy(less)**
- **Throughput=Number of send packet – Number of recevied packet.**

Time slots for packet transmission	Delay (micro sec)
2	154.34
4	792.78
6	1431.56
8	2054.83
10	2486.94

TABLE 1:-DELAY RATE FOR WORMHOLE ATTACK



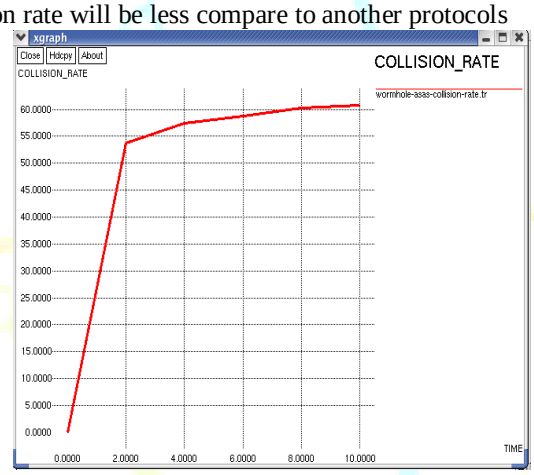
SCREEN SHOT :-3 AVERAGE DELAY IN WORMHOLE ATTACK

In fig:- 9 and above table shows the average delay rate of the nodes with the deployment of wormhole attack in the VANET environment. Lot of denial of services are happen with the wormhole attack .

Time slots for packet transmission	Collision rate (bps)
2	53.72
4	57.36
6	58.82
8	60.21
10	60.75

TABLE 2:- COLLISION RATE IN WORMHOLE ATTACK

In wormhole attack the collision rate will be less compare to another protocols

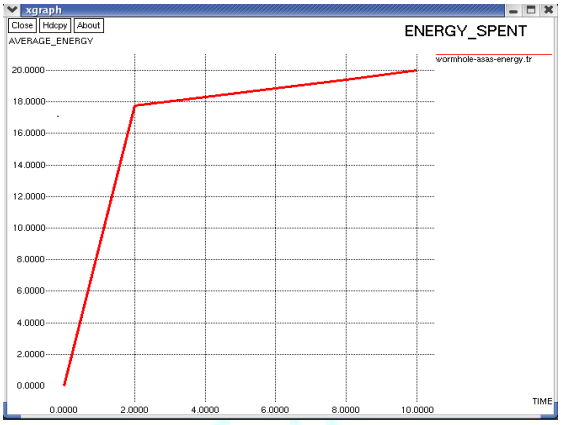


SCREEN SHOT :-4 COLLISION RATE FOR WORMHOLE ATTACK

In fig:- 10 and above table shows the average collision rate of the nodes with the deployment of wormhole attack in the VANET environment.

Time slots for packet transmission	Energy spent (joules)
2	17.74
4	18.29
6	18.26
8	19.42
10	20.00

TABLE 3:- ENERGY SPENT IN WORMHOLE ATTACK

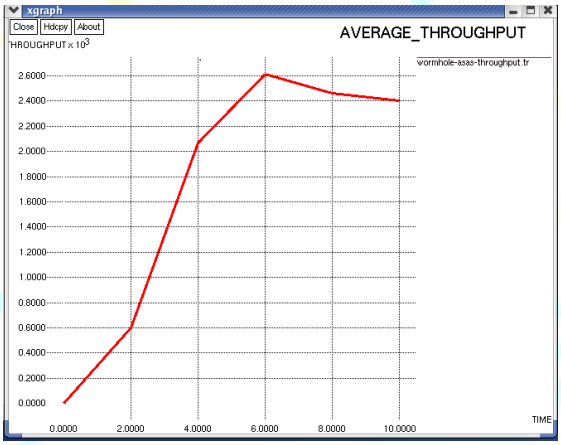


SCREEN SHOT :-5 ENERGY SPENT IN WORMHOLE ATTACK

In fig:- 11 and above table shows the average energy spent in the nodes with the deployment of wormhole attack in the VANET environment.

Time slots for packet transmission	Throughput (kpbs)
2	598.5
4	2068
6	2613.6
8	2461.3
10	2401.05

TABLE 4:- THROUGHPUT IN WORMHOLE ATTACK



SCREEN SHOT :-6 AVERAGE THROUGH PUT IN WORMHOLE ATTACK

In fig:- 12 and above table shows the average throughput rate of the nodes with the deployment of wormhole attack in the VANET environment.

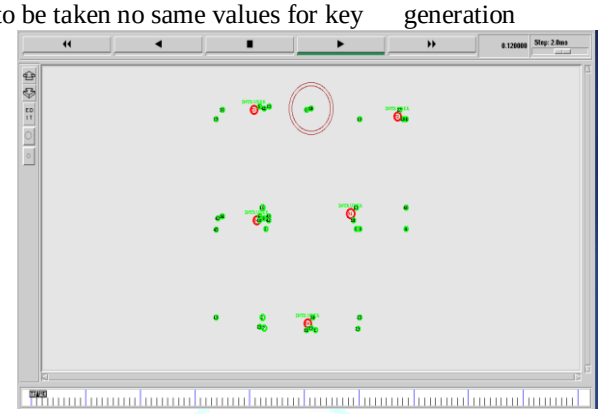
6.2 IMPLEMENTING DIGITAL SIGNATURE AND GAME THEORY APPROACH

Transmission of packets is done using enhanced ASAS-FUZZY with game theoretic approach and digital signature so that wormhole attack is prevented in the network and performance is increased.

DIGITAL SIGNATURE ALGORTHIM

- Generate a random integer.
- The signature must be bit pattern depends on the message being signed.
- Encryption and decryption is done with the public key and private key(with random numbers)

- Signing key verification is done with global components to verify the valid function.
- Random values are to be taken no same values for key generation



SCREEN SHOT :-7 DIGITAL SIGNATURE AND GAME THEORY APPROACH

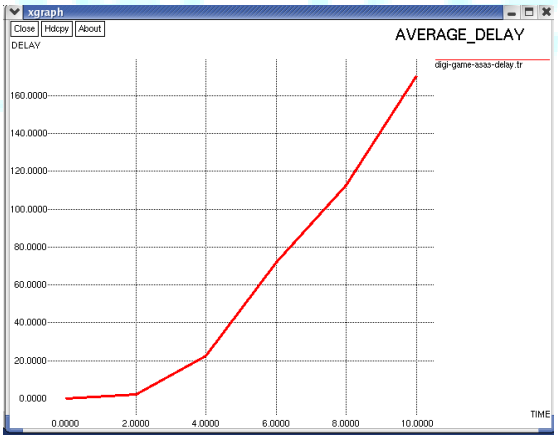
An algorthim problems are stated with the role of players where present in the fig:-13 selected nodes to play typical inputs in the traffic based on that it generate the keys.

SCREEN SHOT :-8 KEY GENERATION

In fig 14 key generation are taken with the random numbers that are chosen in the nodes for communication.

Time slots for packet transmission	Delay (micro secs)
2	1.87
4	22.34
6	71.96
8	112.86
10	170.49

TABLE 5:-DELAY RATE FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

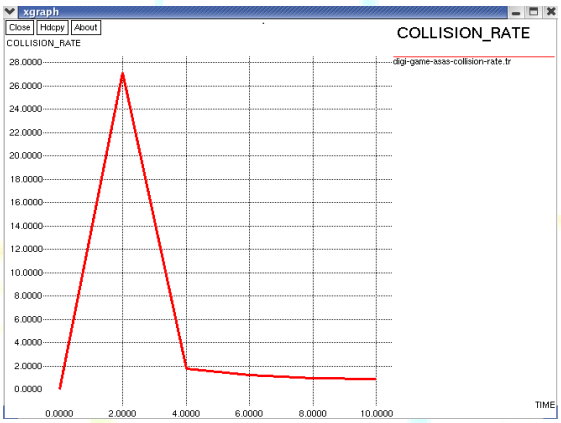


SCREEN SHOT :-9 DELAY RATE FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

In fig:- 15 and above table shows the average delay rate of the nodes with the deployment with digital signature and game theory approach to overcome wormhole attack to in the VANET environment.

Time slots for packet transmission	Collision rate (micro bps)
2	27.14
4	1.772
6	1.189
8	0.954
10	0.908

TABLE 6:-COLLISION RATE FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

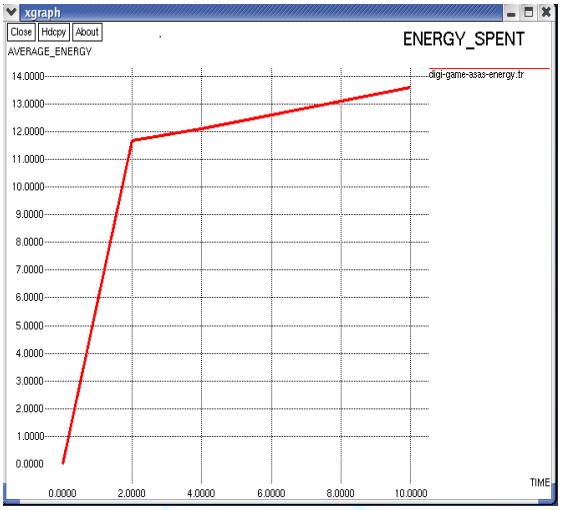


SCREEN SHOT :-10 COLLISION RATE FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

In fig:- 16 and above table shows the average collision rate of the nodes with the deployment with digital signature and game theory approach to overcome collision that present in the wormhole attack.

Time slots for packet transmission	Energy Spent (joules)
2	11.69
4	12.10
6	12.60
8	13.10
10	13.60

TABLE 7:-ENERGY SPENT FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

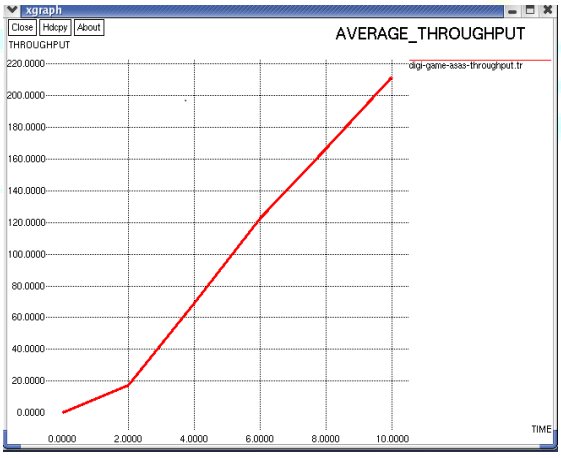


SCREEN SHOT :-11 ENERGY SPENT FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

Eneergy spent in each nodes based on the transmission range to overcome the attacks that happen in the wormhole are taken placed in In fig:- 17and above table shows the average collision rate of the nodes with the deployment with digital signature and game theory approach. Literally compare to the other approaches here it will be more energy drop in the routing mechanism .digital signature reduces the energy spent and increase the ratio of faster communication in the Vehicular environment.

Time slots for packet transmission	Throughput (kpbs)
2	17.52
4	68.91
6	122.93
8	166.88
10	211.90

TABLE 8:-THROUGHPUT FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH



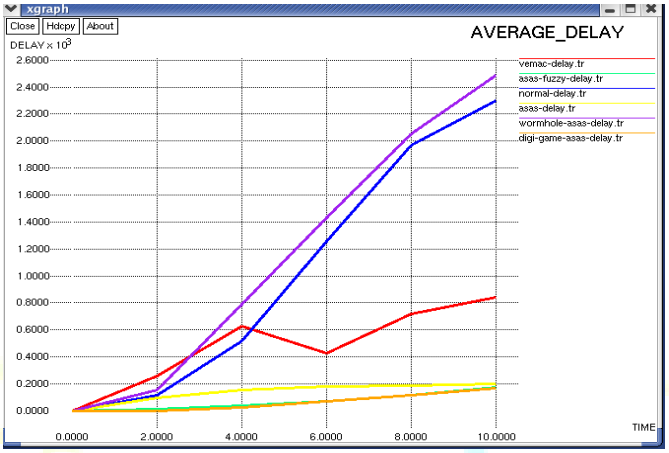
SCREEN SHOT :-12 THROUGHPUT FOR DIGITAL SIGNATURE AND GAME THEORY APPROACH

In fig:- 18 and above table shows the average throughput rate of the nodes with the deployment of digital signature and game theory approach to overcome wormhole attack in the VANET environment

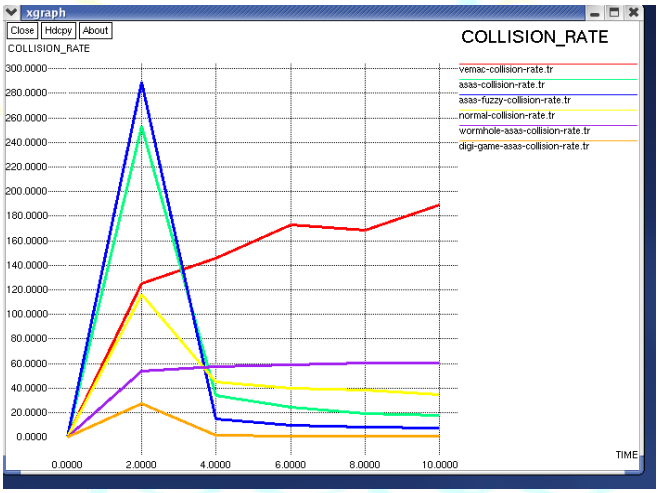
6.3 COMPARISION BETWEEN ESTIMATED VALUES.

ASAS-Fuzzy logics are incorporated with some attacks with normal routing parameter, VEMAC and ASAS protocol with the deploymentation of digital signature and game theory approach with various key generations. QOS parameter are compared with AODV, ASAS ,ASAS-FUZZY ,VEMAC,WORMHOLEATTACK and digital signature & game theory approach is done with output is shown using graphs.

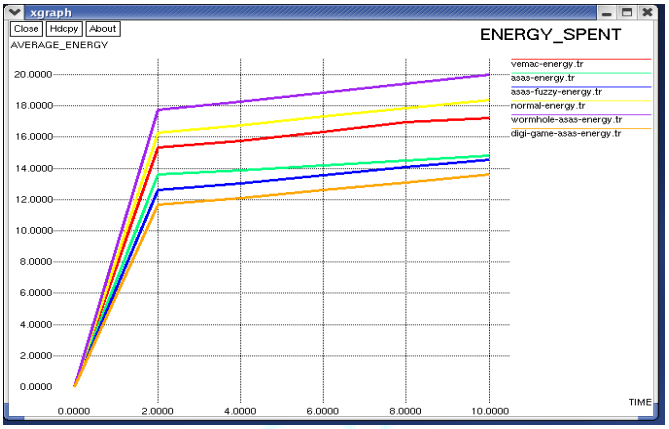
The Graph plot with AODV ,VEMAC,ASAS and ASAS- fuzzy ,WORM HOLE attack and digital signature & game theory using Y graph and time is plotted.



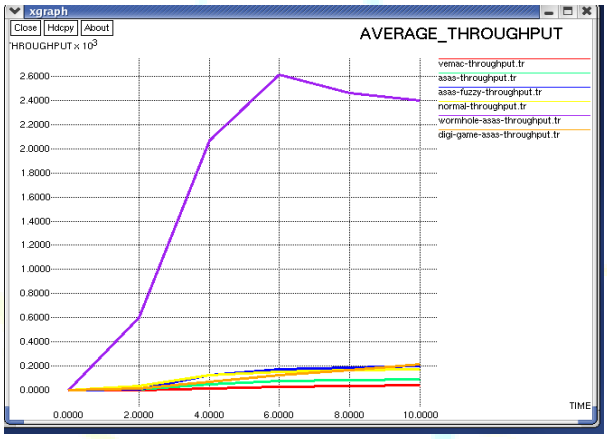
SCREEN SHOT 13:-DELAY RATE



SCREEN SHOT 14:-COLLISION RATE



SCREEN SHOT 15:-ENERGY SPENT



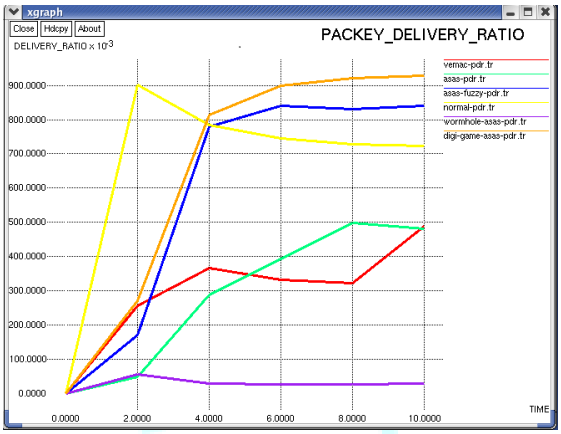
SCREEN SHOT 16:-THROUGHPUT RANGE

In our proposed papers are focussing to reduce the collision is main criteria if we minimize it automatically energy spent to transfer the packet is reduced and increase the through put ratio .In multipath routing mechanism are taken with secure message transmission. Attackers can come from the inside and outside of the node. Road side unit (RSU) contain all information about the vehicles and sends the trust worthy information from the authenticated database in the system.

TIME (secs)	AODV	ASAS	ASAS-FUZZY	VEMAC	WORMHOLE RATE	DIGITAL SIGNATURE AND GAME THEORY
2	0.9024	0.05	0.17	0.2564	0.0553	0.2707
4	0.7842	0.288	0.78	0.3654	0.0293	0.8134
6	0.7461	0.393	0.84	0.3333	0.0272	0.8993
8	0.7276	0.498	0.83	0.3214	0.0275	0.9199
10	0.7228	0.481	0.84	0.4881	0.0282	0.9283

TABLE:9 PACKET DELIVERY RATIO

Above screenshot represent the delay, packet drop in the ASAS-FUZZY environment is deployed with any attacks it shows more number of content modification in the original message Service are to be provided to the system with exceed of the time limit failure of nodes, ring like structure of attack to drop the important information in the environment



SCREEN SHOT 17 :-PACKET DELIVERY RATIO

Digital signature and game theory approach with routing of random variables for typical situation to reduce the attack increase the throughput ratio of this type of scenarios. various key formation are used to enhances the key packet delivery ratio compare to the ASAS-FUZZY based rules in TDMA allocation in VANET.

VII. CONCLUSION AND FUTURE WORK:-

This paper proposes an ASAS-FUZZY based technique with the reserve the channel for vehicles with the TDMA for the VANETs for multiple decision making .It control the various traffic measures with the various speed condition.

Using the shown output result we can analysis the consummation of the collision rate it proven the range of diminution with the increase in the energy during the packet transmission. It is compared with normal AODV, VEMAC, ASAS,and proposed ASAS with fuzzy logics using this we can measure the stability of clustering and increase the packet transmission rate.

In spite of increasing the energy in the vehicles. In future we can build the security between the vehicles to enhance the authentication for communication. For authenticate user roadside unit should be available for the needed packet transformation and to get the non-reputation of the packet. Various attacks are possible in VANETs so track out the adversary with implementing new privacy methods can build for VANETs.Track the adversary with the location based positions.

With the increase of the security to protect the domain with deploying of various attacks it is overcome by the digital signature and game theory approaches in the environment it will reduce the delay in the vehicles . This paper proposes an Digital signature and game theory approach with ASAS-FUZZY based technique for VANET the multiple decision making to provide security in VANET .It control the various traffic measures with the various speed condition.It reduces the delay and increases the packet delivery ratio reduces the various attack in VANET

REFERENCES

[1.] J.Veneeswari, C.Balasubramanian "An urban road traffic with the dedicated fuzzy control system in VANET" ARPN Journal of Engineering and Applied Sciences VOL. 11, NO. 2, JANUARY 2016 .

[2.] Smitha Shivshankar,Abbas Jamalipour:-"An Evolutionary Game Theory-Based Approach toCooperation in VANETs Under Different Network Conditions" IEEE transactions on vehicular technology, vol. 64, no. 5, may 2015.

[3.] Bin Yang, Xiao Sun, Rong Chai, Li Cai, Xizhe Yang-" Game Theory Based Relay Vehicle Selection for VANET" IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Mobile and Wireless Networks 2013.

[4.] Xiaolong Ma, Liangmin Wang-"Game Theory Based Cooperation Incentive Mechanism in Vehicular Ad hoc Networks" International Conference on Management of e-Commerce and e-Government 2012.

[5.] Tomoki Matsukawa, Taisuke Yamamoto, Youji Fukuta-" Controlling Signature Verification of Network Coded Packet on VANET"-2012 .

[6.] Harbir Kaur, Sanjay Batish & Arvind Kakaria-" An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks" International Journal of Smart Sensors and Ad Hoc Networks -2012

[7.] M. A. Alawi, R. A. Saeed and A. A. Hassan, "Cluster-based multihopvehicular communication with multi-metric optimization," ICCCE 2012 ,pp. 22-27, Jul. 2012.

[8.] D. j. Yang, X. Fang, G. l. Xue, "HERA: an optimal relay assignment scheme for cooperative networks," IEEE J. Sel. Areas Commun. , vol.30, no. 2, pp.245-253, 2012.
[9.] M. H. Wei, K. C. Wang, and I. L. Hsieh, "A reliable routing scheme based on vehicle moving similarity for VANETs," IEEE TENCON 2011, pp.426-430,Nov.2011.
[10.] A. Benslimane, S. Barghi, and C. Assi, "An efficient routing protocol for connecting vehicular networks to the Internet," Pervasive and Mobile Computing Journal, vol. 7, pp.98-113, 2011.
[11.] M. Seyfi, S. Muhaidat, J. Liang, and M. Uysal, "Relay selection in dualhop vehicular networks," IEEE Signal Process. Lett. , vol. 18, pp.134– 137, 2011.
[12.] Y. Jiang, H. Zhu, M. Shi, X. Shen, and C. Lin, "An efficient dynamicidentity based signature scheme for secure network coding," Computer Networks, vol.54, pp.28-40, 2010.
[13.] C.-C. Chen, S. Y. Oh, P. Tao, M. Gerla, and M. Y. Sanadidi, "Pipeline Network Coding for Multicast Streams (Invited Paper)," in Proc. 5th Int.Conference on Mobile Computing and Ubiquitous Networking (ICMU 2010), April 2010.
[14.] Y. Bi, L. Cai, X. Shen, and H. Zhao, "A cross layer broadcast protocol for multihop emergency message dissemination in inter-vehicle communication," IEEE ICC 2010, vol.10, pp.88-105, Oct. 2010.
[15.] J. Yoo, B. S. C. Choi and M. Gerla, "An opportunistic relay protocol forvehicular road-side access with fading channels," IEEE ICNP 2010, pp.233-242, Oct. 2010.
[16.] Shea, C., Hassanabadi, B., Valaee, S: "Mobility-based clustering in VANETs using affinity propagation". In: IEEE Globecom (2009)
[17.] T.K Mak,k.pLaberteauxR.sengupta and m-ergen,"Multichannel medium access control for dedicated short range communication ", IEEE transaction on vehicular technology ,vol 58.issuse 1,pp.349-366,Jan 2009.
[18.] CAR 2 CAR Communication consortiums. Http://www.car-to-car.org/.
[19.] The FCC DSRC (Dedicated short range communications) website. http://wireless.fcc.gov/services/its/dsrc/.
[20.] Vanetmobisim project, home page. http://vanet.eurecom..fr.Accessed 29 May 2010.